RELATÓRIO

Atividade criminosa online no Brasil

4º trimestre / 2020

+ year-in-review

São Paulo, 21 de janeiro de 2021

Principais números deste relatório

Clique no número de página após o dado para ir à seção correspondente.

99,2%

foi o aumento dos **casos de phishing** de 2019 para 2020
— página 4

397,4 mi

de credenciais expostas foram detectadas
— página 13

45,4%

dos cartões de crédito e débito expostos na web e detectados pela Axur são brasileiros
— página 18

- **34 arquivos de malware** detectados, quatro a menos do que no trimestre anterior — página 9
- **41,1% de phishing** foram voltados para o e-commerce em 2020 — página 7
- **8,1 caracteres** é o tamanho médio das **senhas vazadas** detectadas — página 15
- **98,93%** dos cartões expostos estavam **dentro da data de validade** no momento da detecção — página 17
- **65%** dos ataques de phishing são feitos sem menção a marcas no domínio — página 8
- **Uso indevido** de marca em buscas pagas **cresceu 11,4%** entre 2019 e 2020 — página 21

A última seção deste relatório, sobre a atividade criminosa em deep e dark web, é de **acesso exclusivo a clientes da Axur**. Por listarem canais, tipos de infração e setores que são alvos dos cibercriminosos, esses dados são sensíveis e centrais em estratégias de segurança digital.

PANORAMA

2020: um ano do qual ninguém esperava sair ileso

Enfim, 2021. É tempo de olhar para o que ficou para trás, sempre com humildade intelectual e dispostos a aprender com os preciosos dados sobre ataques, ameaças e fraudes virtuais que a plataforma Axur identificou.

O último relatório de 2020 tem como objetivo refletir sobre o real impacto da pandemia a curto prazo, no que se refere ao último trimestre do ano, e a médio prazo, já que temos material para analisar o tão falado aumento da superfície de ataque, resultado da pandemia que se instalou no mundo.

Muitas vezes, as informações que nós coletamos causam espanto, mas jamais desanimo. Significa que estamos à frente, olhando para o que nos espera nos próximos meses e, enxergando as tendências do cibercrime no ambiente brasileiro enquanto ainda são desenhadas.

Com os indícios do que vemos para o futuro, conseguiremos continuar entregando soluções que aumentem a segurança digital para nossos clientes e para a sociedade da informação. Isso nos dá a sensação de dever cumprido em relação ao nosso propósito: tornar a internet um lugar mais seguro.

Como eu sempre digo - e você já deve ter lido isso em relatórios passados: "os cibercriminosos evoluem na mesma medida - ou até mais rápido - que a sociedade". Isso quer dizer que, como praticantes da cibersegurança, precisamos estar sempre na frente dessa evolução, precisamos entender o movimento da massa criminosa na web antes mesmo deles se moverem.

No geral, temos uma boa e uma má notícia. Fico pensando em qual você gostaria de ler primeiro. Se fosse eu, a má notícia. Então vamos à ela: 2020 registrou um aumento considerável nas atividades cibercriminosas em relação a 2019, mas até aí, nada além do esperado. No entanto, o último trimestre do ano, registrou uma diminuição que esperamos ver em 2021.

Espero que esses dados tão cuidadosamente coletados e analisados tenham valor para proteção da sua marca e da experiência digital dos seus clientes. Como sempre, seguimos à disposição para ajudar você ao longo dessa empreitada.

Fábio Ramos, CEO da Axur

Phishing

No último trimestre de 2020, a plataforma Axur identificou **8.569 casos de phishing.** Este dado é animador, considerando que representa uma considerável **queda de 18,52%** em comparação aos 10.517 registrados no trimestre anterior.

Mesmo com a queda acumulada no trimestre, a Black Friday 2020 foi responsável pelo pico do trimestre, em novembro, com 3.398 casos de phishing, representando um aumento de **16,82%** em relação à Black Friday de 2019. Em comparação com o mesmo período de 2019, o quarto trimestre de 2020 teve uma irrisória, mas animadora queda de **2,42%** no número de phishings.

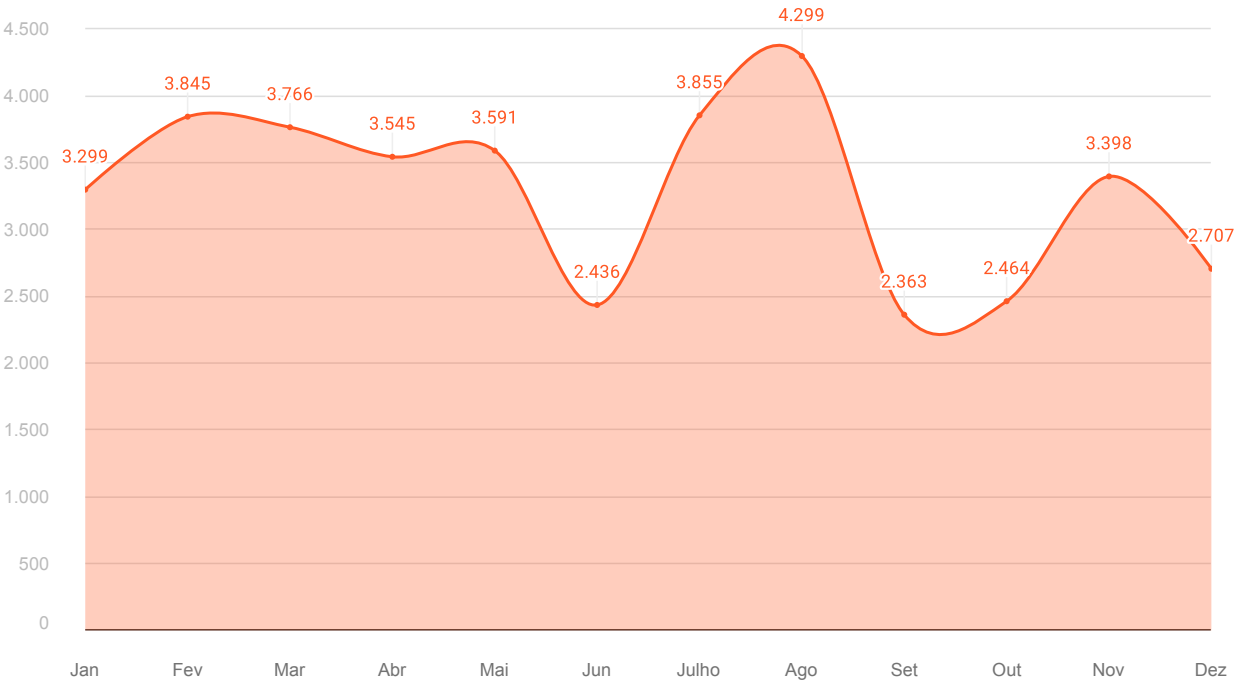


Figura 1. Evolução do número total de casos de phishing detectados no Brasil entre o quarto trimestre de 2019 e o quarto de 2020.

O número de casos acumulados no ano também é digno de atenção. Ele pode, inclusive, indicar uma tendência para 2021: em comparação com os 24.161 casos de phishing registrados em 2019, os 48.137 identificados em 2020, representam um aumento notável de **99,23%**, isto é, quase o dobro de casos de um ano para outro. (Figura 2.). Portanto, é de se esperar que em 2021 tenhamos esse ritmo acelerado no crescimento do phishing, como já temos falado durante o ano todo.

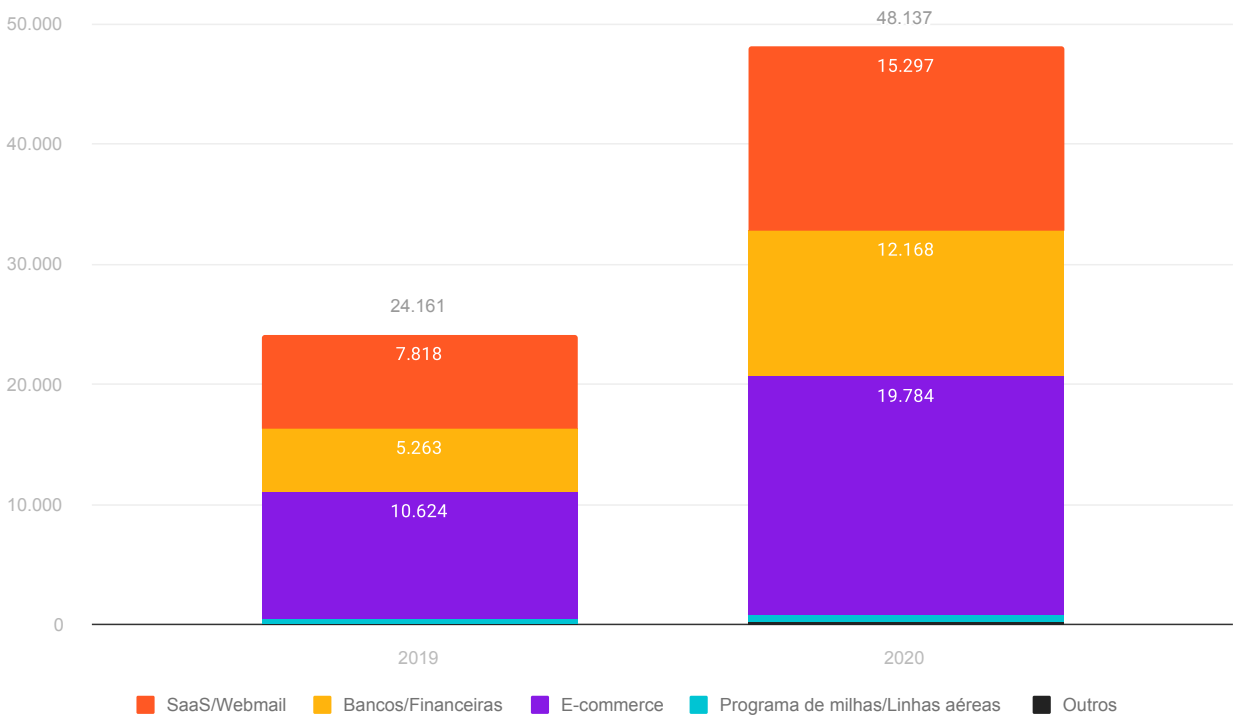


Figura 2. Crescimento anual de casos de phishing por segmento.

O maior destaque do crescimento de phishing do trimestre, assim como no trimestre anterior, é no setor de e-commerce, líder no número de ataques entre outubro e dezembro (Figura 3) e contabilizou, no total do trimestre, **45%** do volume de phishing.

Esse valor indica uma leve queda no setor, que ocupava fatia de 53,5% no trimestre anterior, mas continua firme como alvo de phishing. (Figura 3).

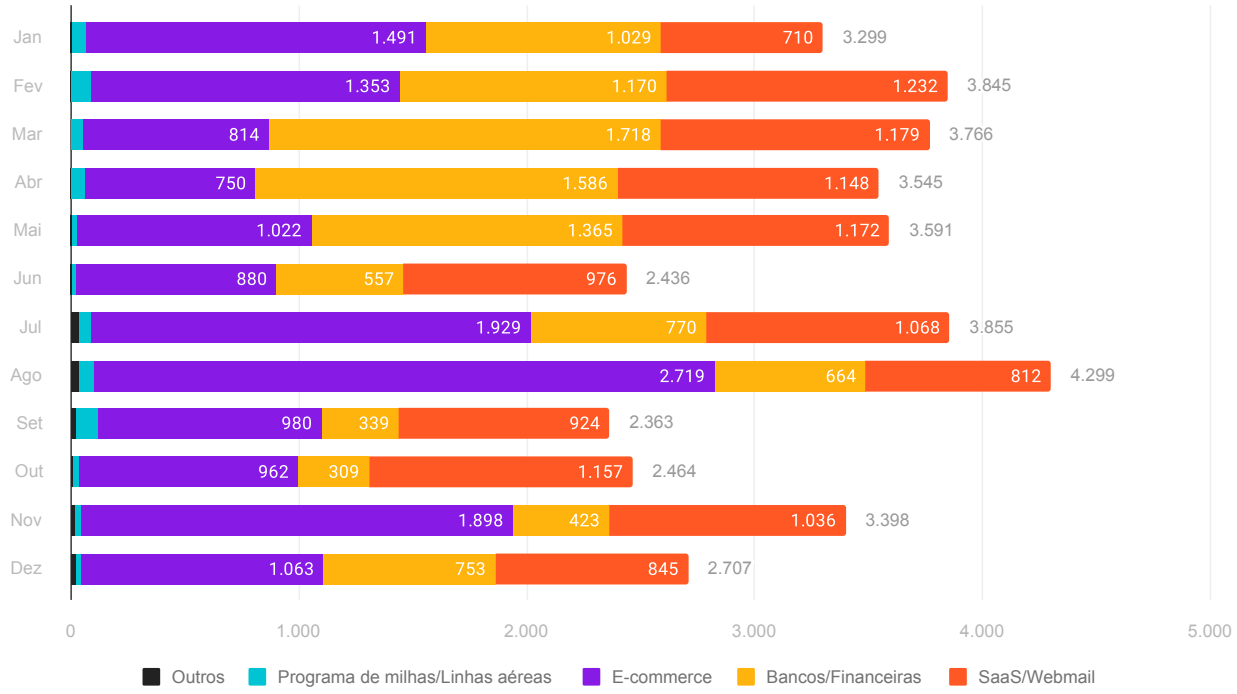


Figura 3. Casos de phishing detectados por mês em 2020, separados por setor atingido.

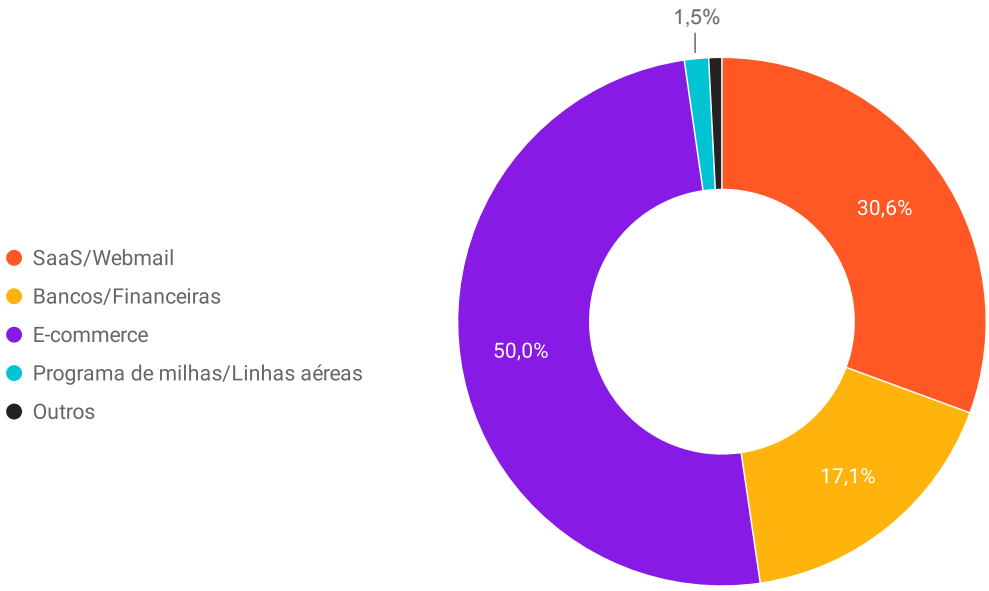


Figura 4. Porcentagem total do número de fraudes de phishing atingindo cada setor de indústria no terceiro e no quarto trimestre de 2020 no Brasil.

No acumulado do ano, o setor de e-commerce liderou, com **41,1%** dos casos de phishing. Considerando o total de 48.137 casos, essa porcentagem indica 19.784 casos só no setor. Isso pode ser explicado pela diminuição de compras em lojas físicas, por conta da pandemia (Figura 5).

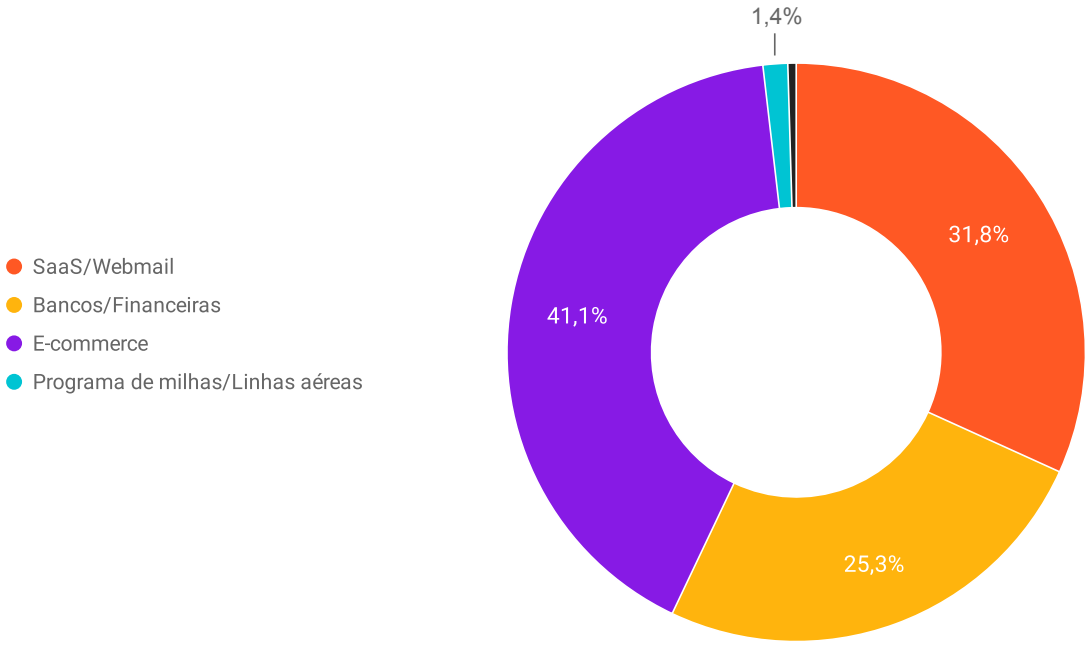


Figura 5. Porcentagem de casos de phishing no acumulado de 2020, por segmento.

Quanto aos nomes de domínios utilizados para phishing, observamos um padrão que se configurava nos meses anteriores. O terceiro trimestre registrou recorde do total de casos com nomes de domínios genéricos, sem menção a marcas e que visam dificultar detecções.

Nesses casos, são usadas palavras como “atualize”, “aproveite”, “ofertas” e outros termos que também podem fisgar mais vítimas. Outra conclusão relevante que podemos chegar de acordo com os dados analisados é a inversão entre uso de domínios similares com domínios genéricos.

Em 2019, como consta na Figura 6, o padrão de comportamento dos cibercriminosos era a utilização de domínios similares a marcas, ocupando **67%** das amostras

coletadas pela plataforma Axur.

No entanto, no último trimestre do mesmo ano, houve desaceleração da prática, tendência que se confirmou no ano de 2020. O pico de utilização de domínios genéricos foi no último trimestre de 2020, com **65%.**

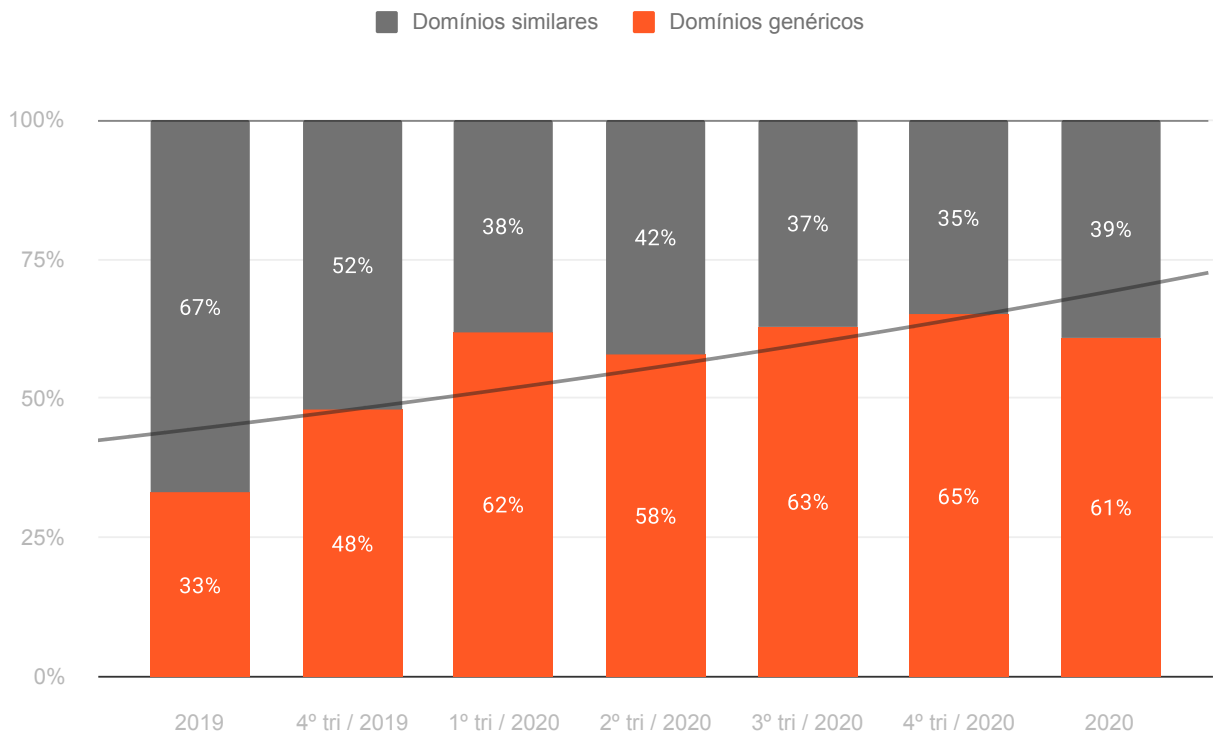


Figura 6. Porcentagem dos ataques de phishing com uso de domínios similares a marcas ou uso de domínios genéricos entre 2019 e o quarto trimestre de 2020.

Malware e trojans

No quarto trimestre de 2020, foram identificados **34 malwares** únicos que afetaram diferentes instituições financeiras. Lembrando que, todos os malwares são do tipo trojan banker, ou seja, nesta análise não foram computados ransomwares e outros tipos de artefatos.

O volume bruto de artefatos de malware demonstra curva decrescente em diminuição em 2020, principalmente se comparado ao pico de novembro de 2019. O segundo semestre de 2020 registrou pequena alta a partir de junho, mas que evoluiu para outra curva de diminuição com novo aumento em dezembro. (Figura 7).

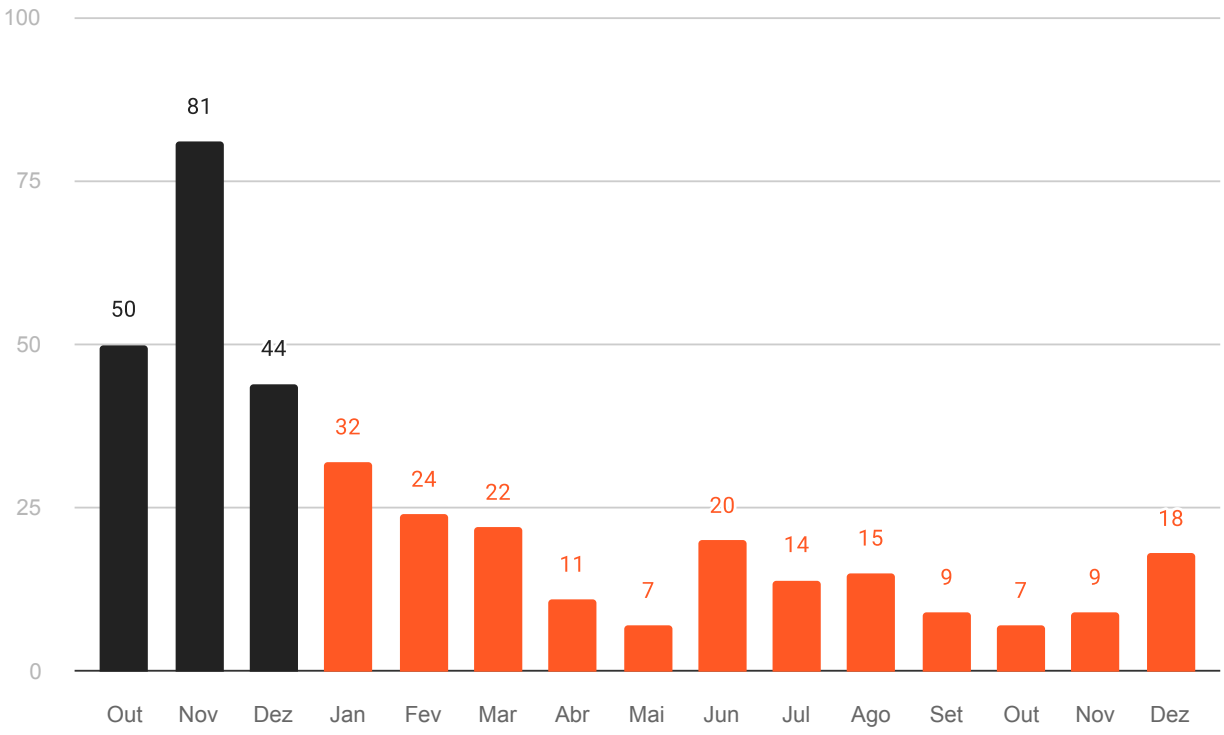


Figura 7. Volume mensal de casos únicos de malware detectados entre o quarto trimestre de 2019 e o quarto de 2020.

Os números médio e máximo de bancos e instituições financeiras detectadas por arquivo estão diminuindo (Figura 8), sem nenhum recorde registrado como no trimestre anterior. É verdade que houve uma recuperação notável em outubro de 2020, quase equiparando-se ao mesmo período em 2019. Seguido, no entanto, de uma aguda baixa em novembro.

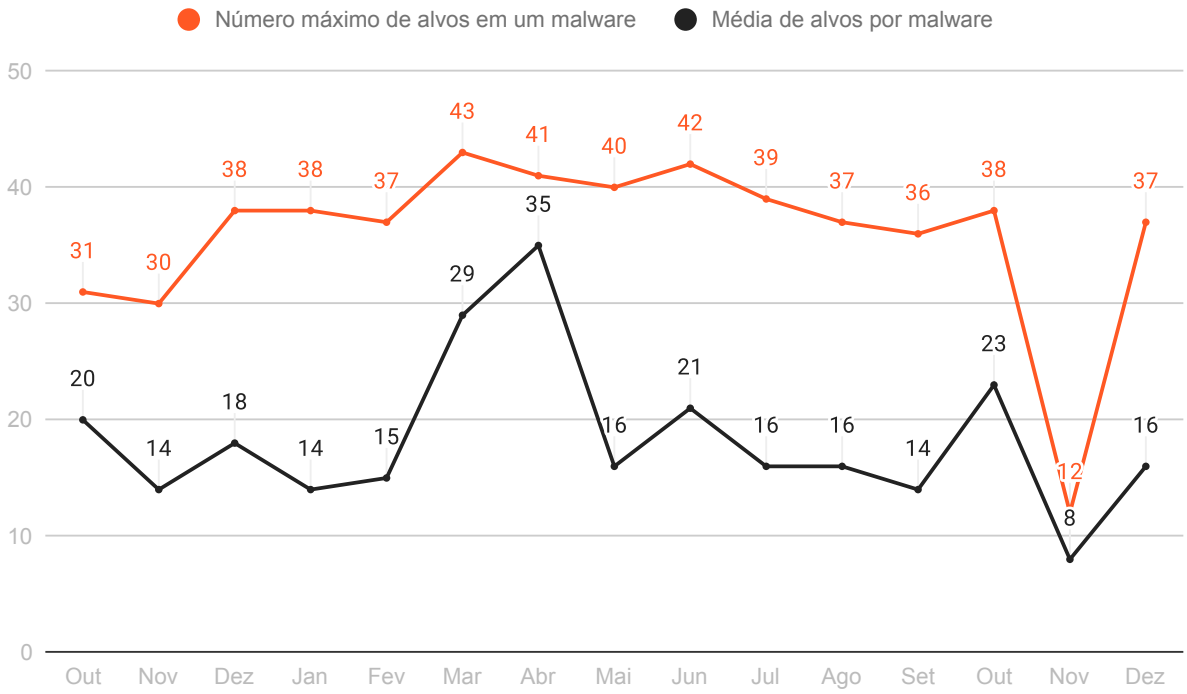


Figura 8. Média e número máximo mensal de bancos e instituições financeiras afetados por malware em 2020.

Quanto à qualificação dos arquivos de malware, temos uma novidade no quarto trimestre de 2020: não houve sequer um artefato do tipo .exe, indicando uma possível tentativa de não chamar a atenção dos usuários e/ou de não serem bloqueados.

Os tipos de arquivos .msi e .cmd foram destaques para os serviços de nuvem da Amazon, que se manteve como principal superfície de ataques (Figura 9).

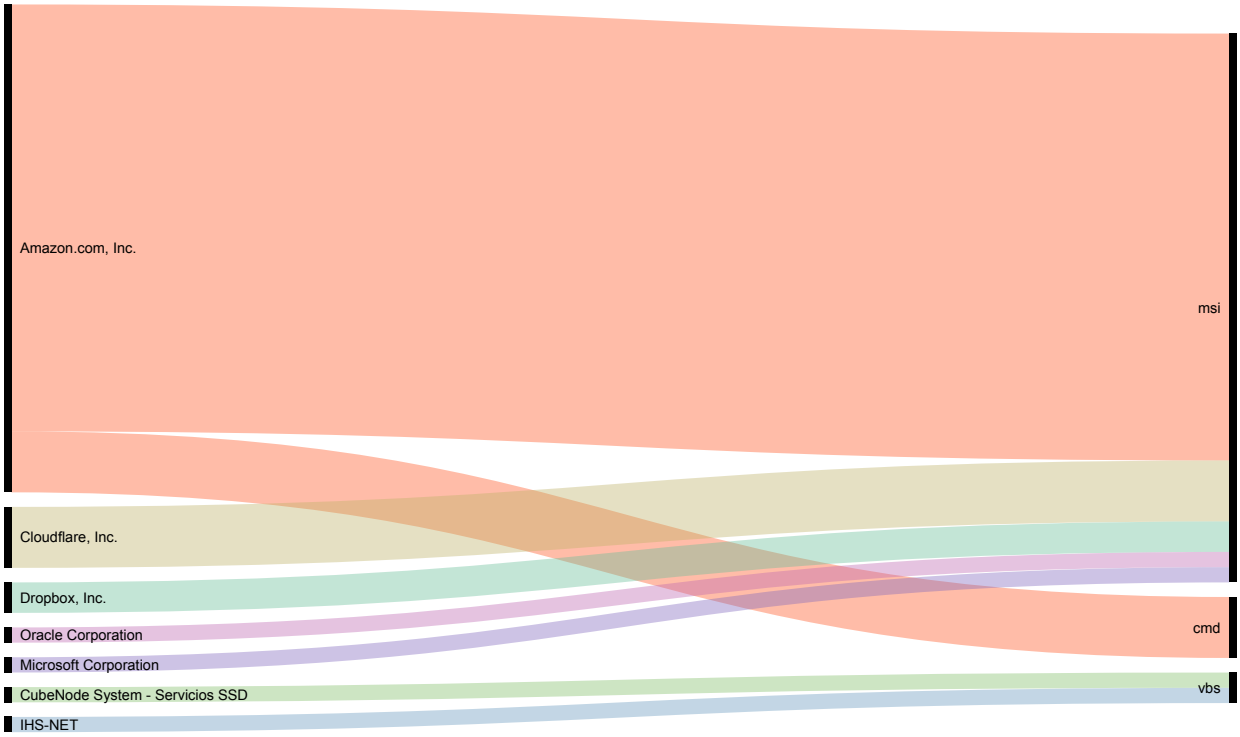


Figura 9. Classificação por ISP de hospedagem e por formato dos arquivos de malware do quarto trimestre de 2020 detectados no Brasil.

Em relação ao acumulado do ano, podemos observar Amazon Web Services, Dropbox, Microsoft Azure e Google Cloud foram isolados os servidores com maior volume de ataques.

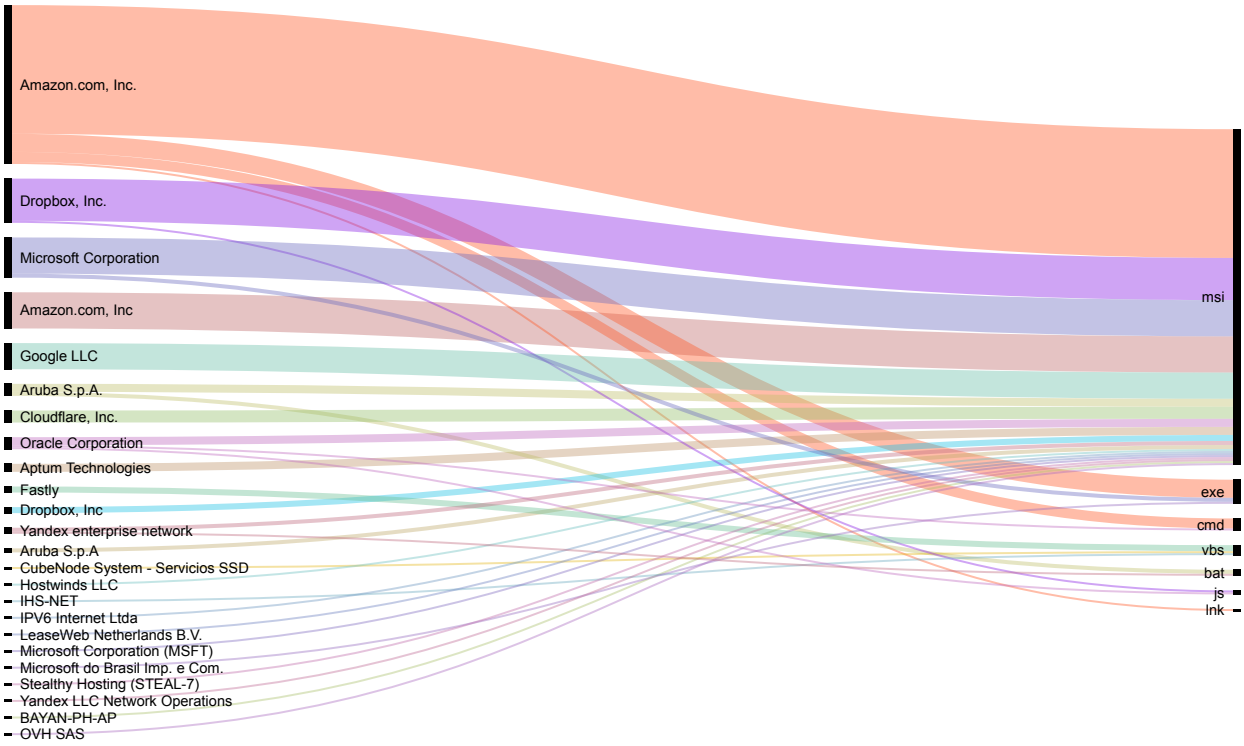


Figura 10. Classificação por ISP de hospedagem e por formato dos arquivos de malware de 2020 detectados no Brasil.

Vazamento ou exposição de credenciais

12,48 milhões é o número de credenciais expostas detectadas pela Axur no quarto trimestre de 2020.

Em 2020, foram **397,42 milhões** de credenciais expostas detectadas.

A variação durante o ano todo (Figura 11) se deve principalmente à distinção de origem dos arquivos de vazamentos. Volumes grandes se referem a bases que contêm, sozinhas, milhões de credenciais (Figura 12)

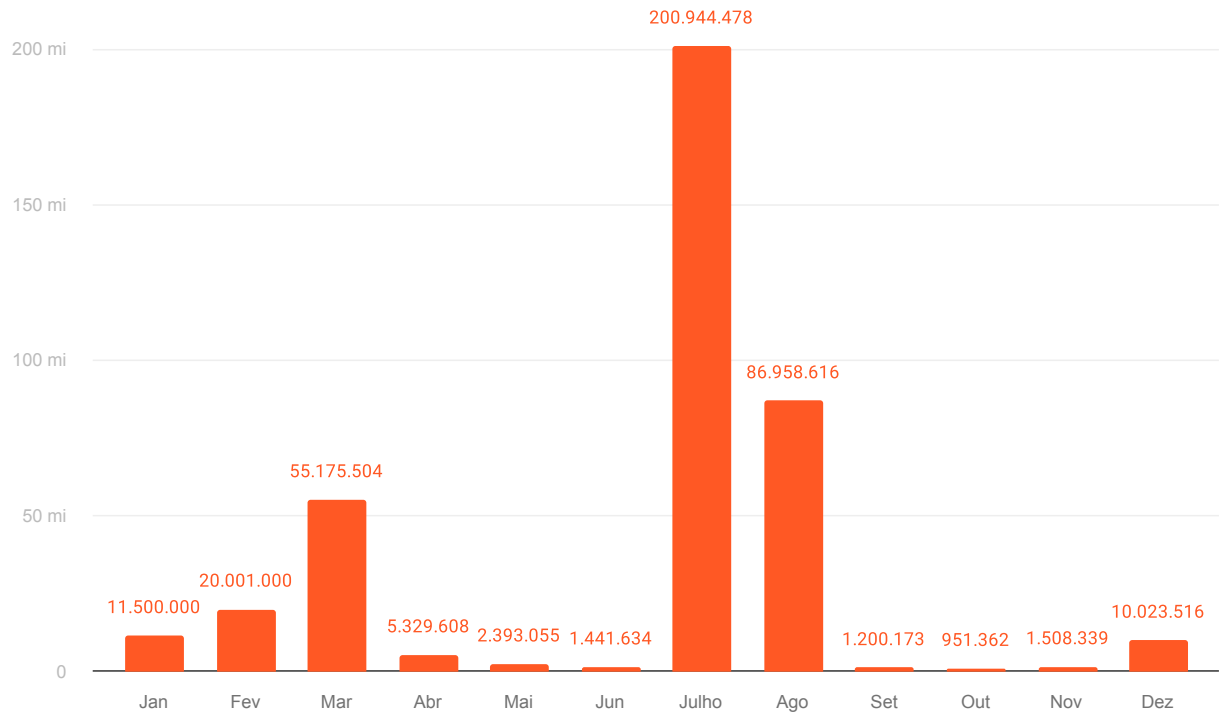


Figura 11. Volume mensal de credenciais expostas detectadas pela Axur em 2020.

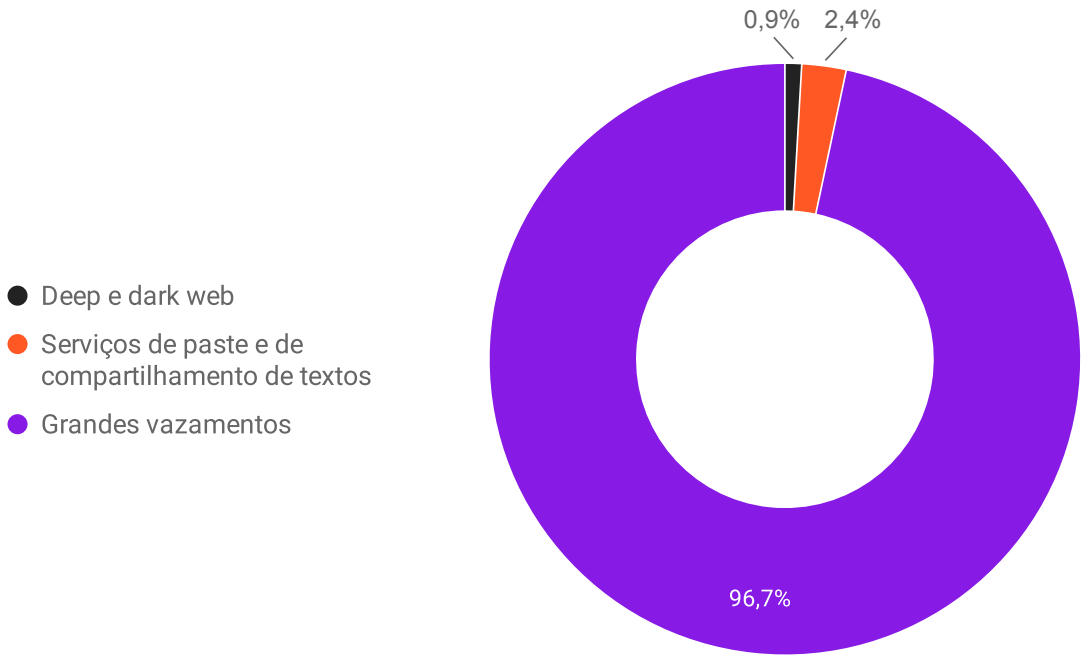


Figura 12. Origem das credenciais expostas encontradas pela Axur em 2020.

No quarto trimestre, foram identificadas:

- **1,09 milhão** de credenciais de domínios corporativos[1] (8,79% do total), distribuídas entre 374.557 empresas distintas afetadas (no total mundial).[2]
- **66.022** credenciais .br, distribuídas em 7.464 domínios distintos.[3] Dessas, foram:
  - **12.858** credenciais de domínios corporativos (19,47% do total

[1] As credenciais corporativas detectadas não necessariamente dão acesso aos sistemas e bases internos das empresas, pois podem apenas ter sido vazadas a partir de cadastros feitos em outros sites com e-mails dessas empresas.

[2] O número de domínios distintos de empresas é obtido a partir da remoção de todos os domínios considerados públicos (como gmail.com, yahoo.com e outros).

[3] As credenciais .br são apenas uma amostra para análise do cenário brasileiro, já que muitos usuários e empresas do Brasil utilizam domínios .com ou outros.

brasileiro, **mais que o dobro do total mundial**), em 7.454 empresas distintas afetadas

- **7.557** credenciais .gov.br distribuídas em 1.656 domínios distintos

Em 2020, foram:

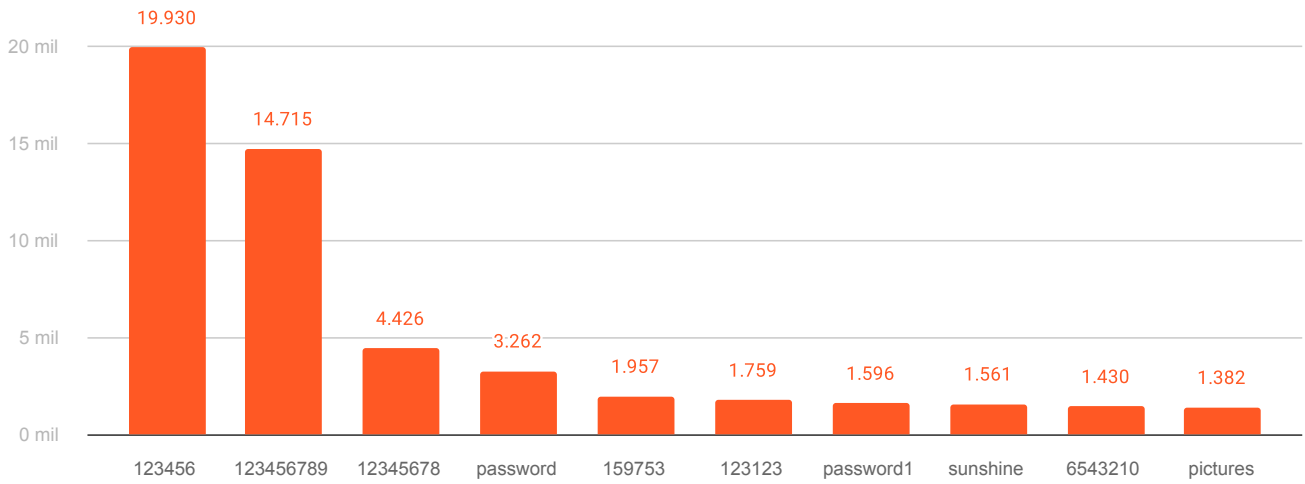
- **31,74 milhões** de credenciais de domínios corporativos (7,98% do total)
- **15,43 milhões** de credenciais .br (3,9% do total)

A senha campeã em vazamentos continua sendo 123456, sequência numérica mais comum tanto no trimestre quanto no ano todo (Figura 13).

O tamanho médio de todas as senhas detectadas no quarto trimestre é de **8,1 caracteres**, maior que os 7,5 do trimestre anterior e semelhante aos 8,3 do segundo trimestre.

Diferentemente do trimestre anterior, as senhas mais vazadas voltaram a ser aquelas compostas somente por letras minúsculas, contabilizando 77,8% do total detectado (Figura 14). No terceiro trimestre, as senhas que continham caracteres especiais somaram 55,1% do total por conta de grandes vazamentos de origem única.

4º trimestre



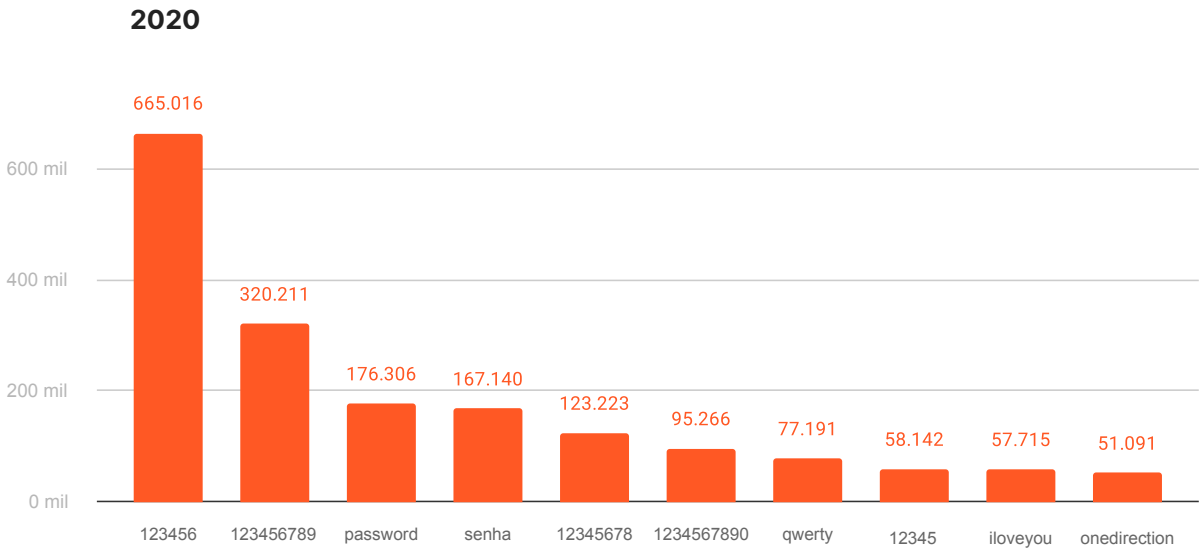


Figura 13. Ranking global de exposição de senhas detectadas pela Axur no quarto trimestre e no ano inteiro de 2020.

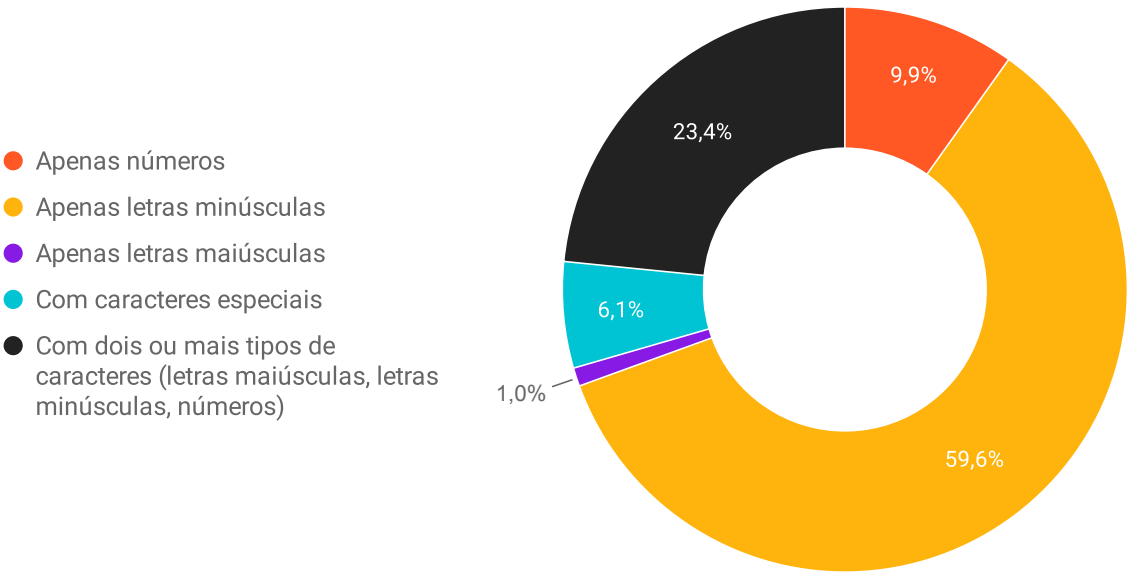


Figura 14. Distribuição percentual de senhas conforme os caracteres que as compõem, identificadas no quarto trimestre de 2020.

Vazamento ou exposição de cartões de crédito e débito

No quarto trimestre de 2020, **325.250** cartões de crédito e débito com dados completos foram identificados pela Axur, expostos da web superficial à deep e dark web e distribuídos entre 17.902 BINs distintas.

Destes, **98,93% (321.773 cartões)** estavam dentro da data de validade no momento da detecção.

Em 2020, foram 2.842.779 cartões expostos detectados.

O número total de cartões detectados no trimestre mostra uma diminuição de **67%** em comparação com o trimestre anterior, quando foram detectados **986.063** cartões.

No quarto trimestre, o Brasil "perdeu" o posto de país com mais exposições de dados de cartões de crédito para os Estados Unidos, em um cenário semelhante ao que aconteceu no segundo trimestre de 2020 (Figura 15). Essa análise é feita com base nas 500 BINs com mais exposições de dados no trimestre.

Na soma das mesmas 500 BINs de cada trimestre, o total anual mostra, ainda assim, que **o Brasil é o campeão em vazamentos de cartões de crédito e débito em 2020** (Figura 16), contabilizando sozinho 45,4% do total mundial e se posicionando com mais de 10 pontos percentuais à frente do "atual campeão" Estados Unidos.

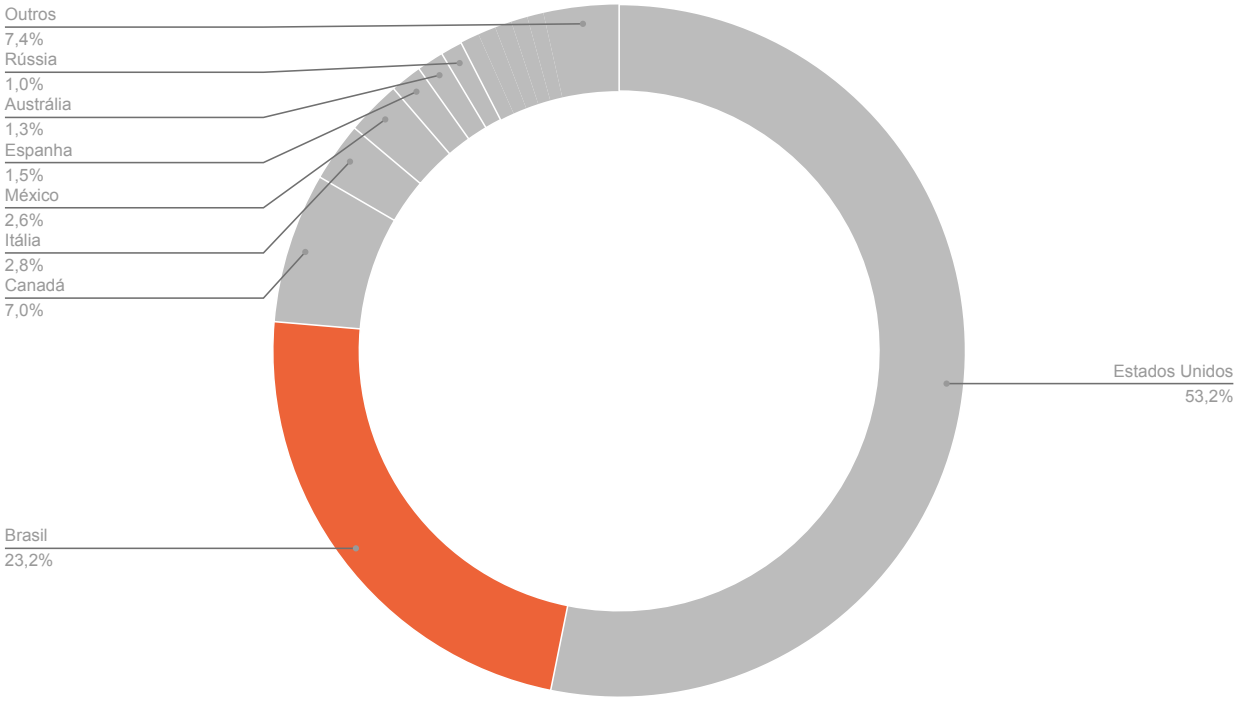


Figura 15. Porcentagem total dos países com mais cartões de crédito e débito vazados online e detectados pela Axur no quarto trimestre de 2020.

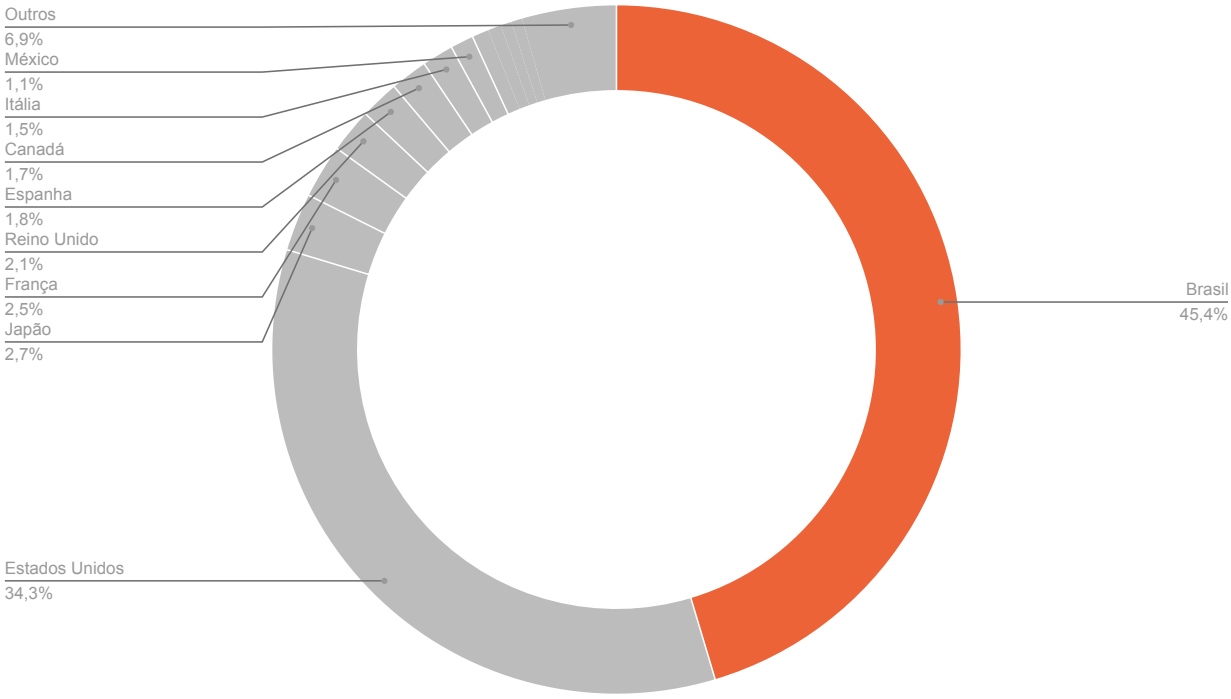


Figura 16. Porcentagem total dos países com mais cartões de crédito e débito vazados online e detectados pela Axur em 2020.

Quanto à origem das BINs mais expostas, no quarto trimestre a campeã em exposições vem do Canadá (Figura 17). Esse é um fato inédito, já que as BINs de outros períodos vêm todas dos “sempre campeões” Brasil e Estados Unidos. Neste mesmo ranking, os Estados Unidos ocupam 5 de 10 posições.

No ano inteiro de 2020, os Estados Unidos têm a BIN com mais vazamentos detectados. Neste ranking, entretanto, a presença maior é do Brasil, com 7 das 10 primeiras posições (Figura 18).

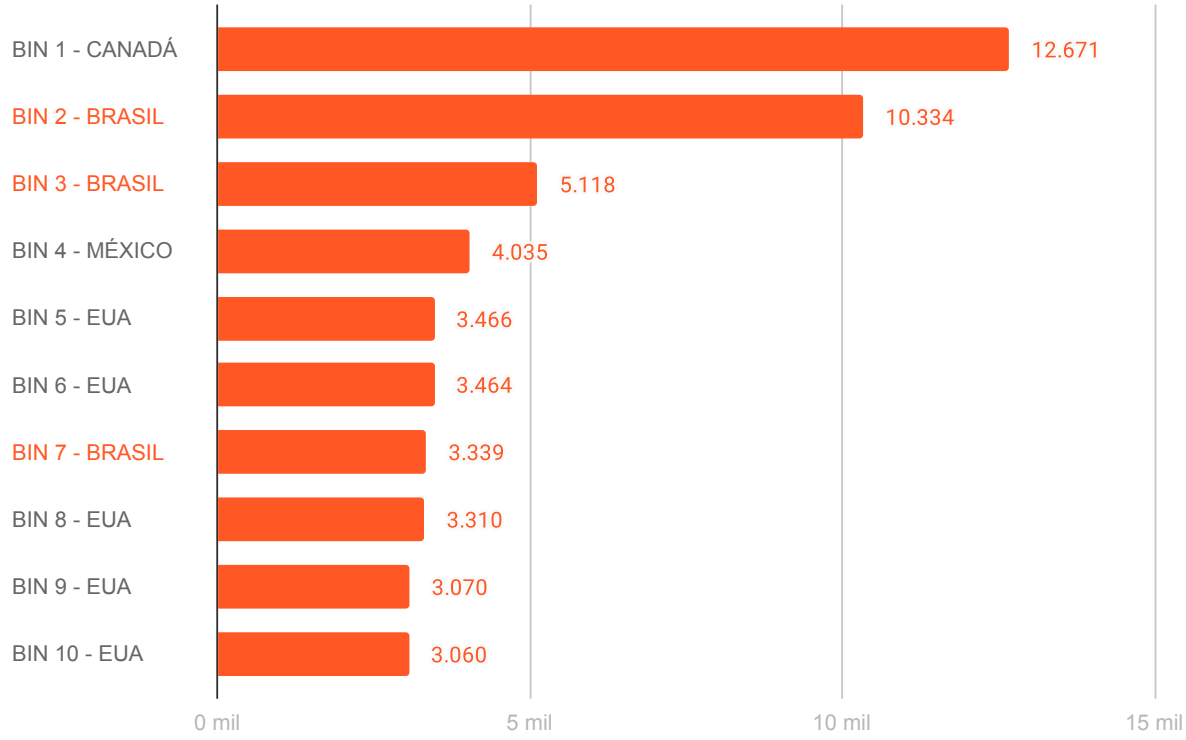


Figura 17. Ranking mundial das 10 BINs com mais exposições de dados de cartões de crédito e débito registrados no quarto trimestre de 2020, identificadas por país.

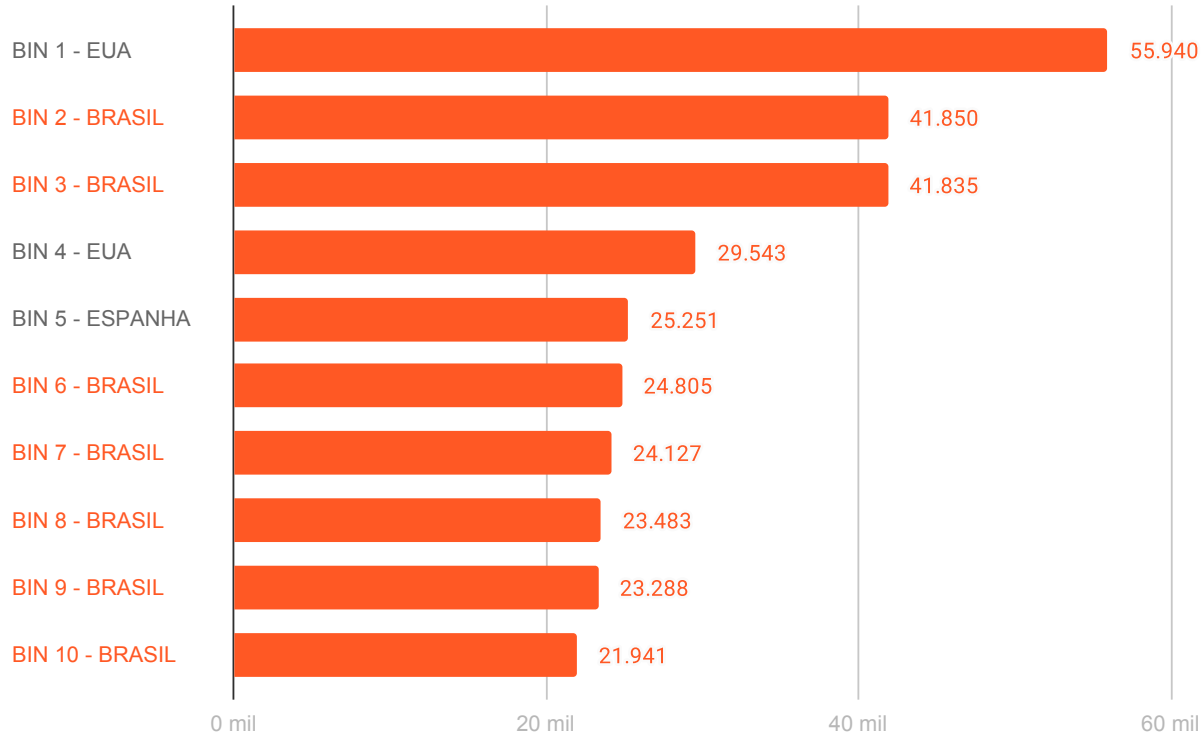


Figura 18. Ranking mundial das 10 BINs com mais vazamentos de cartões de crédito e débito registrados em 2020, identificadas por país.

Infrações em uso de marca

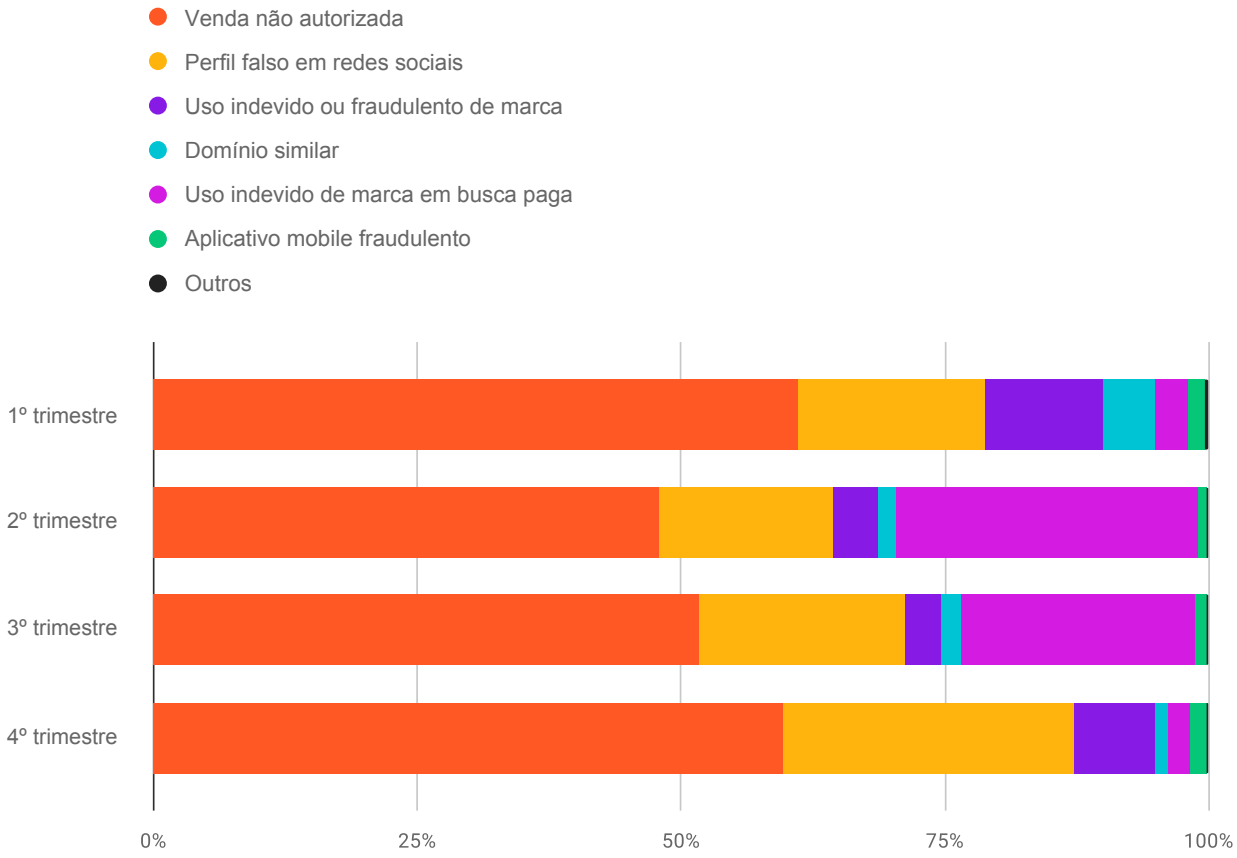


Figura 19. Porcentagem total de incidentes de uso de marca em cada trimestre de 2020.

Usos de marca no quarto trimestre de 2020 mostraram movimentos diferentes: em comparação com o período anterior, houve crescimento percentual considerável de pirataria digital/vendas não autorizadas (de 51,8 para 59,7% do total de cada trimestre) e de perfis falsos em redes sociais (de 19,4 para 27,6), como mostra a Figura 19.

Houve também redução considerável no percentual de infrações em buscas pagas (anúncios nos resultados) do Google e do Bing, que pulou de 22,2 para 2,1%. Essa predominância de incidentes em redes sociais e em vendas não autorizadas pode estar relacionada à intensificação das compras de fim de ano e datas como Black Friday e Natal.

Ainda assim, no total de 2020 foi destaque o crescimento do percentual de usos indevidos de marca em buscas pagas em comparação com 2019 (Figura 20).

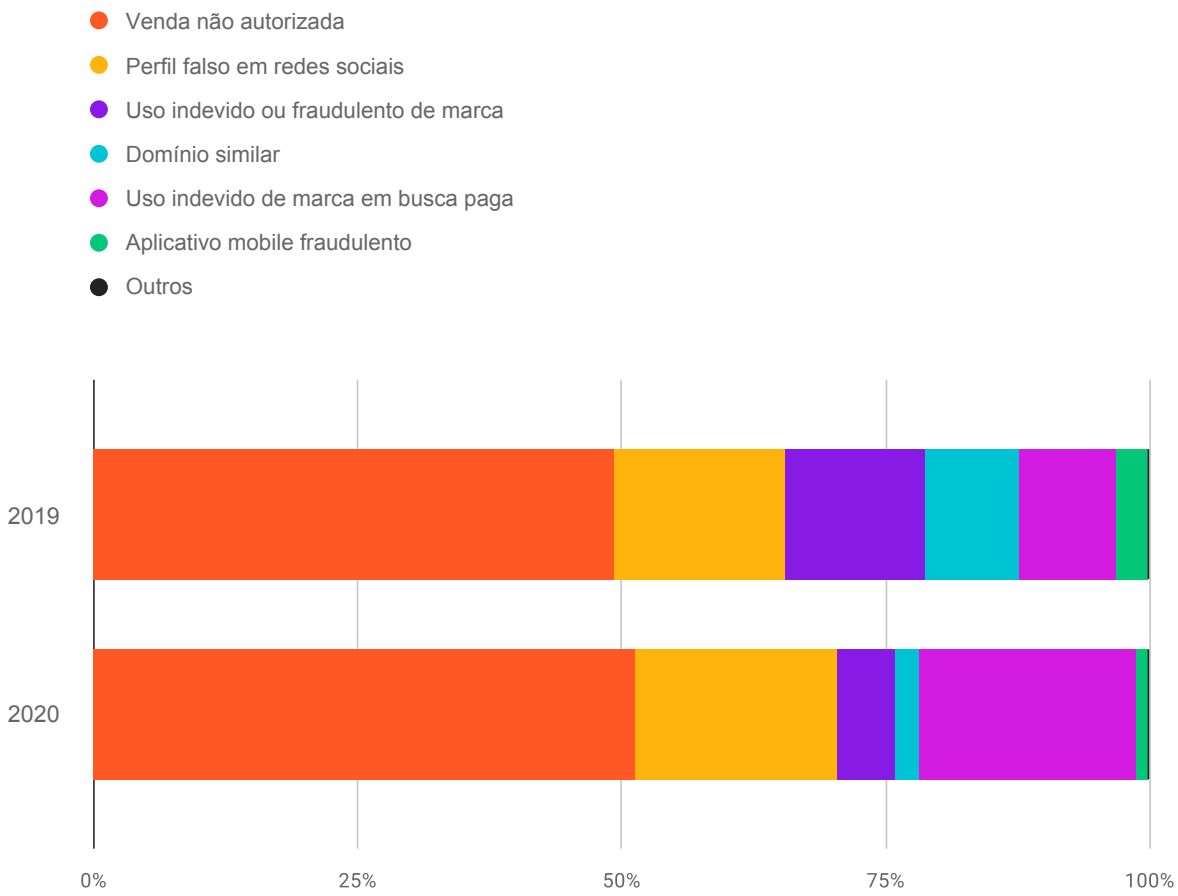


Figura 20. Comparativo de percentuais dos usos de marca encontrados pela Axur no Brasil entre 2019 e 2020.

Detecção e procedimentos

Todas as informações aqui apresentadas foram obtidas a partir do monitoramento diário de milhões de URLs e artefatos maliciosos realizado pela Axur.

As detecções são feitas em web superficial, deep e dark web, e com o uso de tecnologias que permitem que os processos sejam automatizados e mais facilmente visíveis na forma de dados:

- ✓ **Coletores**

  A Axur possui uma estrutura de coletores próprios com todas as possíveis fontes de sinais (milhões de e-mails considerados spam são processados diariamente, e cerca de 780 milhões de URLs avaliadas todos os meses).

- ✓ **Machine learning**

  É usado pela Axur para diminuir exponencialmente os tempos de detecção. O procedimento é feito a partir da análise dos componentes de URLs, de elementos no conteúdo das páginas e do uso de visão computacional, permitindo a identificação de padrões que são ensinados e testados – possibilitando os mais elevados níveis de acertos.

Com essas técnicas, a Axur consegue entregar resultados com precisão, fazendo com que seja possível visualizar ameaças em potencial e incidentes de forma prática e clara. Todas as detecções acontecem na plataforma Axur One, onde é também possível realizar as ações de tratamento.

Para saber sobre as detecções de sua marca e/ou conhecer os produtos de proteção contra riscos digitais da Axur, entre em contato conosco.

Glossário

- **BIN (Bank Identification Number)**
  Os seis primeiros dígitos de um cartão de crédito ou débito, que identificam a instituição financeira emissora e o tipo de cartão

- **Credencial**
  E-mail com senha ou hash (tipo de senha criptografada)

- **Dark web**
  A web acessada somente por navegadores específicos, como a rede TOR.

- **Deep web**
  É a web não acessível via mecanismos de busca e indexação (como o Google).

- **Hash**
  Resultado da aplicação de uma função matemática em algum conteúdo – como senhas.
  É feito para evitar o armazenamento em texto claro e direto, criptografando-o e garantindo mais segurança. Assim, quando uma senha é inserida em um site que usa esse tipo de sistema, o dado é transformado em hash e comparado com o que já está previamente armazenado.

- **Malware**
  Software malicioso que é instalado em computadores, disseminado por técnicas de engenharia social, e que em geral personificam marcas financeiras para capturar dados sensíveis de consumidores.

- **Phishing**
  Site falso e fraudulento enviado com o intuito de capturar dados pessoais, como senhas e números de cartão de crédito.

  - **Spear phishing**
    Forma de envio de phishing direcionada a uma pessoa ou empresa específica.

- **Risco digital**
  Perigos que geram prejuízos financeiros e estão fora do perímetro de atuação da empresa.
  Em termos técnicos, tudo o que acontece fora das proteções de firewall.

Acesse o dicionário de riscos digitais em nosso blog e veja mais!

Sobre a Axur

Líder em monitoramento e reação a riscos digitais na internet, com foco em criar experiências digitais mais seguras para empresas e seus consumidores. Utilizando automações e *machine learning*, monitoramos a web superficial e a deep e dark web para oferecer proteção contra riscos como uso abusivo de marca, apropriação de identidade, phishing, aplicativos fraudulentos e vendas não autorizadas.

Para mais informações, visite axur.com e conheça o blog Deep Space, blog.axur.com.

Contato para a imprensa

Amanda Abed
+55 51 3012 2987
press@axur.com

Endereços

EUA
535 Mission Street – 14th floor
San Francisco, CA 94105

Singapura
109 North Bridge Road
Cityhall District, 179097

Brasil
Rua Mostardeiro, 322 – 15º andar
Porto Alegre, RS 90430-000

axurbr Axur AxurBrasil AxurBrasil AxurBrasil Axur